MEDICAID Y2K PROJECT

HCFA ISSUE PAPER:

Preserving Year 2000 (Y2K) Assets to Benefit Future Medicaid Implementations

March 14, 2000

States invested significant funds and personnel resources in efforts to achieve Year 2000 (Y2K) compliance before the millennium rollover. This paper identifies the Y2K products and processes that are reusable on future projects and should be institutionalized, not archived. Just as States are winding down their Y2K activities, they are faced with preparing for an even larger effort to implement Health Insurance Portability and Accountability Act (HIPAA) standards that will require extensive changes to existing systems, business processes, and, potentially, organizational structures. This paper uses the immediate challenge of HIPAA implementation to illustrate how the products and processes created for Y2K provide an excellent starting point from which to launch any major project.

Preserving Year 2000 (Y2K) Assets to Benefit Future Medicaid Implementations

The purpose of this paper is to assist States in identifying reusable business processes and products that were created en route to Y2K compliance and which provide a starting point for launching any major program initiative. Because Health Insurance Portability and Accountability Act (HIPAA) implementation is the most significant change currently faced by States, it will be used throughout this paper to illustrate lessons learned from the Y2K experience that can be leveraged and retooled to support this massive undertaking. This paper assumes a general understanding of the sections of the HIPAA rules that address administrative simplification and, primarily, Electronic Data Interchange (EDI) transaction formats, standard codes, the National Provider Identifier (NPI), security, privacy, the definitions of entities required to comply with HIPAA, the timeline, and penalty provisions. Even though the implementation dates for HIPAA standards continue to be postponed, now is the time to assess the impact of the changes, consider alternative implementation strategies, designate a HIPAA team, and develop a strategic plan. The assessment effort will not be wasted even if there are more delays or changes in the final standards.

The Y2K experience was one of the largest undertakings focused on a single hardware and software problem the nation and world have ever seen. Systems and infrastructure of every type were examined to determine if the millennium rollover would have any impact or cause a disruption in services. States assessed their systems, renovated and tested them, and coordinated with data exchange partners who were working toward the same deadline. States also learned that Y2K was, above all, a business problem, not just a system bug. As a result of the extensive time and resources the Medicaid enterprise devoted to Y2K compliance, there were virtually no disruptions of any consequence during Day One.

As States are transitioning from Y2K to HIPAA and other major systems projects, they should look at the activities and products that made their Y2K efforts successful and identify good practices that can be leveraged to support the new wave of HIPAA projects. Weak areas in a State's approach to Y2K readiness must be improved to meet the requirements of HIPAA. States have different options for becoming HIPAA compliant. They can choose to replace or renovate the current system, install translators, use clearinghouses, or employ a combination of these strategies. Regardless of the approach chosen, the processes and products used in Y2K projects are valuable assets that can be used to jumpstart the HIPAA project.

This paper has two main sections: Reusable Y2K Processes and Reusable Y2K Products.

REUSABLE Y2K PROCESSES

This section of the paper illustrates how processes developed or used to meet the Y2K deadline apply to the implementation of HIPAA and any future program changes. Processes discussed are:

- Executive Oversight
- Project Management
- Certification and Compliance
- Quality Assurance (QA) and Quality Control (QC)
- Configuration Management (CM)
- Independent Verification and Validation (IV&V)

In general, States exhibiting strengths in these areas were ready sooner, showed self-confidence in the outcome, and demonstrated widespread awareness of the undertaking. States lacking in executive direction and solid management got a later start, were less organized, and had a more stressful experience in their efforts to get ready on time.

Executive Oversight

High-level direction on the part of the governor or the head of the department is the key ingredient associated with success and a low risk rating as reported to the Health Care Financing Administration (HCFA) by its Medicaid Y2K IV&V (hereafter, Y2K IV&V) contractor. Conversely, absence of executive involvement is often cited as an issue contributing to the higher risk status of a State in its Y2K efforts. Many States came to understand the importance of executive oversight spanning the Medicaid enterprise, which includes eligibility systems, payment systems, Managed Care Organizations (MCO), other agencies, providers, and beneficiaries. Executive involvement is essential to ensuring interagency cooperation, availability of adequate funds and resources, establishing priorities, resolving critical issues, and providing direction to the project.

States should build on this successful formula or make improvements in creating the appropriate level of oversight for HIPAA. A model executive committee for HIPAA would include, but not be limited to, the State's Chief Information Officer (CIO), the Medicaid agency's CIO, the director of the Medicaid agency, other agency directors (eligibility, insurance, finance, administration, information technology, and public relations), the State's comptroller's office, the office of the governor, legislative committees, and representatives from the State's provider associations, clearinghouses, MCOs, and system vendors. Other recommendations for the committee are:

- Include legal counsel to advise on contracts that may have to be written or modified between trading partners, interpret the law, and assess the risk of penalties.
- Be constituted now and become familiar with the aspects of HIPAA most likely to affect the State, the providers, and the beneficiaries.
- Identify the major issues that the Medicaid agency and its data exchange partners will have to resolve.

- Establish and communicate compliance guidelines.
- Issue public announcements.

An adjunct of executive oversight is the ability to communicate and coordinate with all players in the Medicaid enterprise. A critical success factor in Y2K was the ability to work with all affected parties to achieve the project goals. Good practices included the ability to establish and maintain an environment which fostered interaction, coordination, support, and issue resolution throughout the enterprise during all phases of the implementation.

The Y2K experience showed that meetings where the decision makers and business partners were present produced a common understanding of problems faced by the enterprise as a whole and resulted in reasonable solutions. The relationships and understanding formed in these sessions during the Y2K project should be continued into the future. Lessons learned can identify improvements and changes to increase the chances of a successful HIPAA implementation.

Project Management

The approach to project management is a critical component in any project. It provides the basis for the management of the project, guidance on which activities should be undertaken, and the leadership necessary for a successful outcome. The key to the success of any project is the ability of the management staff to adequately control and supervise the project and to make management decisions on issues that arise. The project must be carefully structured, monitored, and conducted, with sufficient flexibility to respond to occasional unforeseen problems. The lack of solid project management was an area of significant risk assessed by the Y2K IV&V Team.

The IV&V Team identified several processes that contributed significantly to the positive outcome in States that had the most success in delivering their Y2K projects. These are:

- Formal project planning with regular updates and a budget
- Action item management
- Change management
- Risk management
- Status reporting conducted on a regular basis and distributed to all team members
- System design and development methodology
- Problem identification and resolution
- Regular internal meetings of the project team

Successful States had written and proven procedures in all of these areas and demonstrated how the good management practices were a part of their culture. Some States lacked documented procedures, but hired contractors who brought in a project management methodology and oversight.

The implementation of HIPAA requirements will require broader coordination of activities, considerably more complex work plans and schedules, greater risk management, and more extensive problem identification and resolution. If the Y2K project was well managed and coordinated, the State is off to a good start and can use its successful methodology. If not, or if

the State contracted for management services, it will have to decide how to improve and institutionalize an approach to management that can meet the demands of HIPAA or determine to contract again for project management services. Examples of HIPAA-specific recommendations in the area of project management are:

- Identify Subject Matter Experts (SME) for each HIPAA standard and transaction to assess impact and requirements.
- Name a security officer and a privacy officer to manage the implementation of new security and privacy regulations.
- Use the same General Accounting Office (GAO) phased approach or similar industry standard to organize the project.
- Use management tools to control and report on progress.
- Develop a strategy document on how to address HIPAA requirements and document reasons for selecting the implementation solution.
- Coordinate the release of information to trading partners and plan well in advance for end-to-end testing.
- Use Y2K procedures for archiving documentation.

Certification and Compliance

Every large project has goals and objectives that define the basis for the work to be completed. For Y2K projects, this meant ensuring that the production systems would not be impacted by the date rollover or associated calculations. In order to validate the remediation effort, methods were put in place to determine the compliance of the systems and to certify that the work was completed. In the most successful States, a high-level definition of compliance was mandated, and organizational units were designated to monitor progress and provide official certification that all modifications were satisfactorily completed. Standardized check-off forms were implemented to ensure uniformity and thoroughness. This provided an external review process and gave the State more assurance that it was indeed ready for the rollover.

The modifications required for HIPAA are far more extensive than the Y2K changes were. However, the organization created to define and monitor Y2K compliance can be used as the starting point for HIPAA certification and compliance. A good practice in some States was the designation of a high-level Y2K Chief. Similarly, a dedicated HIPAA Compliance Officer could be named to oversee all implementation activities, beginning with establishing an approach to the definition of Y2K compliance. Another good practice in defining Y2K compliance was to involve SMEs from the State's information technology department and its Medicaid agency. To establish a definition of compliance for HIPAA requires a thorough understanding of the rules and the implementation strategy selected for the State. It is important that all trading partners concur on the definition of compliance. Partners should also have a mutual sign-off process documenting that compliance has been achieved.

Quality Assurance and Quality Control

The success of any project is directly related to the quality of the work performed. A QA program and QC procedures are needed to validate that the work performed meets the expected

outcomes and standards. This paper focuses on QA and QC in the systems development environment. QA is a high-level discipline established within the organization to ensure customer satisfaction, enforce compliance with standards, and conduct audits applied by specialists *independent from* the project management. A documented QA plan and procedures and a dedicated professional staff are essential.

QC can be a process identified within the QA program. It is the function of inspecting products and services after they are produced to verify that they are up to standard. QC staff can be part of the system development organization or user group, but must be separate from the staff that did the work. QC includes standard procedures for testing modified code, conducting walkthroughs, performing documentation review, and tracking corrections until the product is acceptable.

During Y2K preparations all States used some form of QC, but some were lacking in documentation of the process and the results. More importantly, most lacked an independent QA function. Because of the complexity of HIPAA requirements and the staggered schedule for implementation of the rules, States should seriously consider establishing a QA program that includes an approach to certifying compliance. They should also assess the QC process currently in place to identify areas for improvement, particularly in producing documented procedures.

Independent Verification and Validation

Several States (or their fiscal agents and other venders) engaged IV&V contractors during the course of their Y2K projects. The Y2K Assessment Team considered this practice to be a risk reducer. In addition to internal QC and separate QA, an external IV&V review can assist in keeping a project on course and providing more assurance that compliance has been achieved. IV&V can be an assessment of procedures and products, or it can involve an independent test of functionality. In some States, the IV&V contractor functioned as a partner of the State by providing full management support throughout the project. Given the number and complexity of HIPAA standards and other rules, an IV&V contractor is recommended.

Configuration Management

CM refers to methods for controlling the versions of code in a production system undergoing renovation, the systematic promotion of new code into the operational system, and maintenance of prior versions. CM includes configuration identification, configuration status accounting, and configuration audits. The Y2K IV&V assessment revealed that several States lacked automated CM processes. In these States, tracking who was working on which version of a program was primarily a manual process based on the staff's expertise in maintaining the system.

A robust CM process will be even more important with HIPAA. As currently planned, there are a number of staggered implementation dates for HIPAA standards, with only a few months in between. For example, system changes made to implement the NPI are likely to be implemented after the same software has been modified to accommodate the new EDI transactions and standard codes. Different teams may be assigned to implement different standards, but all will be working on the same application programs. This is a potential source of confusion, as databases and software applications will be subject to waves of changes. States will not be able to manage

HIPAA changes without a strong CM program that includes a documented plan and procedures. Improvements in CM will benefit the State in the implementation of HIPAA standards and in any future systems development projects.

REUSABLE Y2K PRODUCTS

Y2K projects yielded many products that can be assets for the HIPAA implementation. Modifications may be required to improve the products and make them HIPAA-specific, but the time and effort already spent provide a good head start for the HIPAA project. The following reusable products are discussed below:

- Y2K Staff
- Project Plan and Schedule
- Strategic Planning Documents
- Inventories
- Testing and Validation Plans
- End-to-End Test Plans
- Automated Tools
- Outreach Plans
- Communication with MCOs
- Web Pages
- Business Continuity and Contingency Plans (BCCP)
- Other Products

Y2K Staff

Staff assigned to Y2K planning and management activities represent a resource of experience which the State should consider as its primary asset in planning for HIPAA or any major enterprise-wide project. Individuals learned valuable lessons in executive oversight, outreach to providers and beneficiaries, planning of comprehensive end-to-end testing, and developing BCCPs, all of which contributed to the success of the 2000 rollover. States should carefully assess the staffing plans used for Y2K and consider assigning leadership and support staff with the most experience in Y2K to the HIPAA project.

Project Plan and Schedule

The basis of any project is the project plan. The Y2K project plan can serve as a starting point for HIPAA, especially in the use of phases and the initial activities of assessment. The same systems, and many of the same tasks and activities, will be required for HIPAA. The resources assigned to complete these items may be the same as in the Y2K project. States that had thin project plans (i.e., lacking in details of tasks, assignments, and dates) will have to dramatically improve the quality of the project plan in order to meet the HIPAA deadlines. The HIPAA project plan and schedule will necessarily be much broader. The complexity of the HIPAA implementation calls for use of a project-planning tool. There should be a plan and schedule for each HIPAA standard and transaction, as well as an integrated plan for the entire project.

Strategic Planning Documents

The Y2K IV&V assessment identified good practices in those States that documented and published their approach to strategic planning. Examples of these documents are:

- Renovation strategy
- Certification plan and strategy
- Risk management plan and strategy

Although the content of such documents will be different for HIPAA, the format, approach, and approval plan should be evaluated for reuse. Because of the penalties riding on a failure to meet HIPAA standards and dates, legal counsel should review all statements made in the renovation strategy, certification plan, and risk management documents.

Inventories

At the beginning of the Y2K project, all States undertook the major task of assessing their systems, data exchange partners, equipment, Computer-Off-The-Shelf (COTS) products, hardware, Data Centers, databases, operating systems, buildings, and infrastructure. The focus for HIPAA implementation is on the Medicaid Management Information System (MMIS) application software, telecommunications and network management, and all interfaces with external trading partners. During Y2K preparations, States conducted detailed assessments of their systems and interfaces to identify valid source code components, eliminate outdated programs, and identify and count the lines of code and fields affected by the date change. The inventories completed for Y2K provide a baseline for HIPAA, but the States will need to build upon the baseline because there are many more fields to assess, including, but not limited to:

- Number of fields using the provider ID
- Size and composition of the current provider ID (especially if it contains embedded logic)
- Number of system functions and databases using the provider ID as key to the business rule (e.g., number of claims edits, rate tables, MCO primary care physician cross-references, payment calculations, HCFA reporting routines, or Surveillance and Utilization Review Subsystem (SURS) provider class grouping)
- Number of system functions and databases using local codes as key to the business process (e.g., local code is associated with a payment formula)
- Creative (non-standard) use of procedure code modifiers
- Number of system functions and databases impacted by new EDI standards
- Number of years of claim (and encounter) history requiring conversion
- Number of new transaction formats to implement or cross-reference throughout the system.

In most States, over a million lines of code will have to be analyzed to determine the level of impact of the HIPAA rules. States should seriously consider using automated tools to assist in the inventory and assessment activities.

Testing and Validation Plans

No matter what approach a State takes to achieving compliance with HIPAA regulations or other large-scale mandates, testing of modifications is required to ensure that the system continues to perform the same functions as it did before the changes were implemented. During the Y2K project, levels of testing typical of any system enhancement project were conducted, and test plans, scripts, and results were documented. Future-date testing is not required for HIPAA, but all levels of testing will be far more extensive because changes will be required to all databases and processes involving claim, encounter, and several other transactions, the provider ID, local codes typically used by Medicaid, and security procedures.

In the Y2K risk assessment, States with exemplary test plans and documentation of the testing processes were more likely to be assessed at low risk of failure. Issues were raised with States that could not demonstrate the same level of planning, thoroughness, and accountability. States that demonstrated weakness in documenting the testing process must improve to be successful in the implementation of HIPAA.

While Y2K preparations were focused on date calculations, a number of the most critical business processes were identified and testing scenarios were created to verify that changes did not affect ordinary processing. The test plans, files, and data used for Y2K can be used as the starting point for the HIPAA testing process. While significant additional scripts, data, and scenarios will be needed, the approach to testing key business processes has already been developed.

End-to-End Testing

Many States conducted end-to-end testing in which providers, MCOs, and other critical data exchange partners submitted test claims and encounters as input to the renovated MMIS, and the MMIS exercised all normal processes through to payment and reporting. States varied greatly in the scale of end-to-end testing performed. In some States end-to-end tests were limited to a handful of designated providers or replaced by simulated provider input. Other States encouraged comprehensive end-to-end testing with many providers and set aside additional time at the Data Center so that providers could continue their own Y2K readiness testing.

With HIPAA, it is likely that far more extensive end-to-end testing will be required. For example, all the data exchange partners (including the Medicaid agency and its system contractors, Medicare Contractors and other insurers, enrollment brokers, data warehouse contractors, eligibility verification system vendors, providers, and MCOs) must be HIPAA compliant, or use clearinghouses to convert their claims and other formats. With Y2K there was more tolerance for the providers who were not Y2K compliant because the MMIS could accept non-compliant date fields and apply bridging or windowing techniques. Under HIPAA standards, no data exchange partner can transmit non-compliant data to another (but the trading partners can satisfy compliance by using a clearinghouse or installing translator packages). States can certainly get a head start using their Y2K end-to-end testing strategies. Reusable tools for this approach include:

- Inventory of Electronic Media Claims (EMC), EDI, and Point-of-Sale (POS) providers
- Inventory of all EMC and EDI formats by transaction type
- Inventory of web download providers (e.g., MCOs receiving enrollment data or submitting encounter data)
- Posting of the schedule of end-to-end testing (e.g., provider, date, time, volume), including available hours for open testing
- Instructions to the providers for initiating and conducting the tests
- Procedures for Data Center staff, systems engineers, and provider relations staff to follow during the testing (e.g., staffing plan, activities, reporting, and communications with the providers)
- Schedule for additional resources needed (e.g., Data Center, technical, and program staff)
- Report on CPU usage (as a baseline measure for planning the additional impact of HIPAA testing)
- Record of programs and tables used in the test
- Error report used for the test
- Sign-off process (plan showing the test validation activity and designated persons with authority to sign a document stating that the test was successful)
- Procedure to be followed when a test is unsuccessful and must be rescheduled.

In anticipation of the higher demand on resources and longer time required for end-to-end HIPAA testing, the tools listed above should be assessed for improvement and expansion. Some new processes will probably be needed (e.g., the agency may want to recommend that providers who continue to submit non-compliant data after a certain number of attempts should contract with a service bureau).

Automated Tools

Y2K inspired a proliferation of tools tailored to the needs of the undertaking. States acquired tools through purchase or licensing, or invented their own. Tools were used for the initial assessment of application software and databases, generation of test data, tracking progress, maintaining the status of errors and corrections, and testing. Tools specifically designed to find dates and create future dates will not be useful for HIPAA, but there are many more fields and formats to be identified and analyzed. Automated tools are essential to the efficient completion of the analysis of the impact of HIPAA on the organization and critical to the planning tasks required to manage the project. States should first see if the automated tools used for analysis, testing, and project monitoring for Y2K are reusable for the analysis of HIPAA. The State may need to invest in upgrades or purchase new tools for the HIPAA implementation.

Outreach Plans

Outreach became a major initiative during the Y2K projects. Because of the possibility of problems and the uncertainty of the success of the rollover, States had to communicate with their providers, beneficiaries, and employees. States came to recognize that outreach required a great deal of planning and coordination. In many States, outreach itself and the content of the message were hotly debated and decisions were made at the gubernatorial or department level. Y2K propelled many States into a degree of outreach never before undertaken. In the most successful

States, separate units were responsible for developing and providing the outreach information. Most States created plans for the various types of outreach based on their target audience.

The planning and products developed for Y2K outreach are reusable for HIPAA. Examples include:

- Mailing lists (must be comprehensive; all data exchange partners must be identified)
- Target groupings associated with different types of messages
- Reusable formats and delivery modes; replacing Y2K information with HIPAA information
- Schedule for release of communications (e.g., review the schedule used for Y2K and make modifications to improve effectiveness of communications)
- Number of addresses and cost of transmitting communications
- Media, including web messages, computer-based training, videos, radio, TV, posters, pamphlets, and letters
- Materials used in provider association and community meetings
- Identification of staff who managed the Y2K outreach activities
- Promotion of attendance at local and national conferences and meetings

In the area of beneficiary outreach, the same concerns regarding readiness apply (i.e., if the provider and payer systems fail due to problems associated with the new standards, how will beneficiaries continue to receive service?). At a minimum, States will have to inform all beneficiaries about the new privacy rules, explain what they mean to the beneficiary, and tell what the State has done to implement them.

Y2K was also a sounding board for communications between the State Agency and various contractors, including the fiscal agent, the data warehouse contractor, the enrollment broker, sister agencies, local eligibility offices, pharmacy benefit managers, Value-Added Network (VAN) vendors, and others. The State should review its Y2K communications plan and adapt it for the larger task of communicating with all data exchange partners and standards organizations engaged in implementing HIPAA.

Before initiating the new awareness and communication program, States will probably want to analyze the effectiveness of their Y2K outreach activities. For example, Medicaid staff could contact professional associations to determine the level of customer satisfaction and identify areas that need improvement. There will probably be more interest on the part of the provider community during the implementation of HIPAA standards because all electronic data trading partners must comply, and penalties will be assessed for non-compliance. With the benefit of hindsight, States can improve their outreach practices.

Communication with MCOs

Improved communication with all data exchange partners is critical; however, States should pay particular attention to their MCOs during the implementation of HIPAA. During the Y2K readiness period, a few States demonstrated exemplary practices in communication with MCOs, exchange of information, interface testing, assessing the MCOs' readiness, or certifying the

MCOs' Y2K compliance. In many States, however, very little contact occurred due to concerns over contractual boundaries. There may be time to correct this problem as States enter into new contracts with the MCOs. Under HIPAA rules, both the State Medicaid Agency and the MCO are classified as "health plans." All of the compliance requirements that apply to the Medicaid Agency also apply to the MCO. The MCO is just a smaller model of the State Agency. The MCO exchanges data with providers, other payers, and system contractors. It must meet HIPAA requirements for all of the transactions, NPI, standard codes, security, and privacy. The MCO faces the same problems as the Medicaid Agency in converting to or adopting the new NPI and the use of standard codes.

It is to the benefit of both States and MCOs to get off to a good start in planning HIPAA implementation. If a State has been planning for HIPAA for some time, the agency could offer HIPAA awareness or implementation training to the MCOs. Some States instituted regular meetings with MCOs and produced newsletters during the Y2K implementation. A few States established interdisciplinary committees to cover systems and operational issues. For HIPAA, there could be special committees set up to address EDI transactions, NPI, and privacy requirements.

It is likely that all States will have to revise their contracts with MCOs in order to specify HIPAA-compliant encounter data, eligibility inquiries, enrollment updates, security requirements, and privacy procedures, and to reference the implementation dates after which penalties apply. The new or modified contracts will be complicated by the variety of approaches the State, the MCOs, and the providers contracting with the MCOs will choose for compliance (e.g., renovation, replacement, use of clearinghouses, or use of translators). The State must be fully aware of its own implementation plan and that of each MCO. States should consider broadening the approach to communication with MCOs that was used for Y2K. Examples of Y2K products to be strengthened for HIPAA are:

- Update the MCO contact list to include managers of provider services, enrollment, claims processing, legal counsel, utilization management, prior authorization, security, and privacy.
- Update the list of providers contracting with or employed by MCOs.
- Assess how the MCOs plan to implement changes in their systems and how their systems will interface with the provider community.
- Assess MCOs' outreach efforts to providers and beneficiaries.
- Assess MCOs' ability to conduct end-to-end testing with providers.
- Coordinate efforts for end-to-end testing between the State and all MCOs. It is not likely that all MCOs will be ready for testing at the same time.
- Share BCCPs between the State and the MCOs. There is a high probability that not all parties will be ready on time and, therefore, the BCCP will have to be used.
- Include MCO representation in the HIPAA executive oversight committee.

Web Pages

During the Y2K project, States found that it was necessary to provide broad-based information to a variety of audiences. In order to accomplish this goal and to keep all key information in a single area for public access, many States created web pages and procedures for updating them. The web page will be a valuable medium for communication between the State Agency and its data exchange partners during the implementation of HIPAA. It is likely that the Y2K web page is easily adaptable to HIPAA. Examples of retooling possibilities are:

- Links between the State's web page and key administrative simplification web sites
- Compliance definition and certification process for HIPAA
- Links to web sites for professional organizations and contractors
- Links to high-level summary of the HIPAA administrative simplification rules and standards
- Explanation of the State's approach to compliance with the NPI, security, and privacy
- Master plan and timetable for State implementation of HIPAA
- Posting of end-to-end testing schedules
- Posting of community meetings to discuss HIPAA (or any outreach program)
- Frequently Asked Questions (FAQ) about HIPAA
- Directory of the State's oversight committee or parties responsible for HIPAA implementation, e-mail addresses, and telephone and fax numbers

Business Continuity and Contingency Plans

Due to the extensive modifications required for Y2K and the possibility that problems could occur, States created BCCPs to protect their ability to continue with critical business processes in the event that breakdowns occurred. States are advised not to archive their BCCPs, but rather to review them for their relevance in any kind of major event that threatens the delivery of service and payment to providers.

The magnitude of the HIPAA effort and the fact that it touches all data exchange partners in the Medicaid enterprise suggest the potential for disruption to service or payment due to the failure of State systems to meet the mandated implementation date. The BCCP created for Y2K is an excellent starting point to ensure continuity of service during the implementation of HIPAA. With Y2K, there was a single target readiness date of January 1, 2000, but with HIPAA there are multiple readiness deadlines with no breathing room in between. One of the benefits of creating the BCCP for Y2K is that critical business processes have been identified and prioritized. The information and knowledge gained during these exercises are invaluable to the agency as it plans for HIPAA implementation. Examples of reusable parts of a BCCP are:

- Identification of critical business processes
- Identification of manual workarounds to be used in the event of a system failure
- Identification of key staff and their functions
- Identification of a minimum acceptable level of service

In many States, the BCCP is the only enterprise-wide document available. It encompasses systems and operations, and both internal and external organizations. This document serves as a resource to identify critical processes and interfaces that will be impacted by HIPAA. Managers and supervisors can use the BCCP as input to the HIPAA planning effort, and as a checklist to ensure that all bases have been covered.

Other Products

During the Y2K IV&V assessment, several States demonstrated good practices in the use of system development products such as enterprise models, entity relationship diagrams, and data dictionaries. These products are of value at any time, no matter what program change or system modification is being considered. States that do not have a model of their data exchange partner universe or an automated data dictionary are at risk of overlooking partners and data subject to HIPAA requirements. Also, on-line system documents and user manuals will greatly facilitate the many changes associated with HIPAA standards.

NEW PROCESSES AND PRODUCTS

It is possible that some business process reengineering will be needed to support provider enrollment and the assignment of the NPI, workarounds due to the inability to use local codes, expanded security procedures, and new privacy requirements. The agency may have to reenroll all providers. To meet privacy requirements, States will have to create a privacy unit with leadership, training, and staff, develop a privacy complaint process for beneficiaries, and enforce privacy standards. At a minimum, States should assess the impact of HIPAA rules on their organization and determine where changes are needed to achieve compliance.

CONCLUSION

In general, the Y2K readiness experience was a testing ground for a State's approach to any major, enterprise-wide project. The Y2K IV&V effort identified good practices as well as weaknesses. All States demonstrated significant progress as they approached the rollover. States should consider their Y2K experience to have been a rehearsal for HIPAA implementation or any major project. Executive oversight, project management, and other critical processes and tools addressed in this paper should be mustered, assessed, improved, and deployed for HIPAA and other future challenges. Good practices and lessons learned in the Y2K project are the baseline for success.